BRACKISH SECURITY

PARTNER PROGRAM

FOR MSPS, MSSPS, CONSULTANCIES & AGENCIES

Partnership Models

Two ways to put a senior offensive security team behind your service catalog: white label, delivered entirely under your brand, or straightforward subcontracting, run in our operations portal with your team alongside us. Same testers, same tradecraft — you choose whose name is on the work.

MODELS	DELIVERY	COVERAGE
White Label	Manual-led	Application & API
Subcontract	AI-Augmented	Mobile
	Senior-driven	Cloud
		Secure Code Review
		Red / Purple Team
		AI / LLM
		And more

PREPARED BY

Brackish Security

306 W Redwood St STE 201

Baltimore, MD 21201

WEB

brackish.io/partners

CONTACT

info@brackish.io

00

Contents

Why Partner with Brackish 01

Two Ways to Work Together 02

White-Label Delivery 03

Subcontract Delivery 04

The Operations Portal 05

Reporting & Branding 06

Service Catalog 07

Commercial Model 08

Onboarding 09

Frequently Asked Questions 10

Get Started 11

01 Why Partner with Brackish

Offensive security is the capability your clients ask for most and the hardest one to staff. Experienced testers are scarce, expensive, and difficult to keep busy enough to justify the hire — and a tester kept busy on other work is a tester losing the edge you hired them for.

Partnering solves the capability without the headcount. You keep the client relationship, the contract, and the margin; we bring career offensive-security specialists to the work, in whichever of the two models below fits the engagement in front of you.

100%

Offensive security focus — no split attention across unrelated service lines

Manual

Senior-led exploitation; automation supports our people, never replaces them

Certified

Team holds industry certifications (OSCP, OSWE, OSEP, CISSP), and select personnel hold active U.S. security clearances

NO HIRING, NO BENCH RISK

No recruiting cycle, no training program, no idle capacity between engagements. You take the work when it arrives and we staff it.

BREADTH ON DAY ONE

Web, API, mobile, cloud, internal and external infrastructure, wireless, physical, social engineering, AI/LLM, and secure code review — the whole catalog, not the two things one hire happens to be good at.

CLEAN INDEPENDENCE

As an external firm we give you real tester/developer separation and credentialed personnel — the posture your clients' auditors, customers, and regulators are looking for.

WE DO NOT COMPETE WITH YOU

Offensive security is all we sell. We are not looking to take over your managed services, your helpdesk, or your client relationship.

02 Two Ways to Work Together

The choice comes down to one question: whose brand is on the work in front of the end client. Everything else — the testers, the methodology, the depth of the assessment — is the same either way.

	WHITE LABEL	SUBCONTRACT
Who the end client sees	Your firm, exclusively. We are invisible to them.	Brackish, disclosed as your testing subcontractor.
Deliverable branding	Your logo, your template, your house style.	Brackish-branded, or delivered without branding for you to present.
Where the engagement is run	Your systems and processes. We work inside them.	**portal.brackish.io** — scoping, findings, reports, messaging, and signatures in one place.
Accounts and identities	You provision accounts for the assigned testers under your brand.	None to provision. Testers work in our portal as Brackish staff.
Portal access for your team	Not used for delivery.	Named accounts for your staff, scoped to the engagements they are on.
Client communication	Entirely through your team.	Through your team, or direct with us present as your subcontractor — set at kickoff.
Operational overhead on you	Higher — you own the client-facing surface end to end.	Lower — we run the engagement machinery and you stay in the loop.
Best fit	Testing sold as a standing line in your own catalog.	Senior capacity on a named engagement, quickly, with minimal setup.

The paperwork is the same in both models

A mutual NDA and a partner master agreement between your firm and ours, then a Statement of Work and Rules of Engagement per engagement. Your contract with your client is yours alone — we are never a party to it, and we never invoice your client.

Nothing stops you from running both, either. Partners commonly subcontract the first engagement with a new client to get it moving, then move the relationship to white label once the service becomes a standing part of their catalog.

03 White-Label Delivery

Testing delivered under your brand. Every report and debrief carries your name — to the end client it is a seamless extension of your own services.

WL

Your brand, our testers

You own the client-facing surface; we supply the tradecraft behind it

WHAT WE DO

- Scope the assessment with you and agree its engagement value.
- Execute the testing with senior, career offensive-security specialists.
- Author the report into your template, with your branding.
- Brief your team for the client debrief — or present it as your team, if you prefer.
- Re-test high and critical findings on request within 60 days of final report delivery.

WHAT YOU DO

- Hold the client relationship, the contract, and the pricing.
- Supply the report template and brand assets you want us to author into.
- Provision working identities for the assigned testers under your brand.
- Handle client-facing scheduling and correspondence.

TESTER IDENTITIES UNDER YOUR BRAND

Because the engagement is presented as yours, the testers need to appear as yours: you create the accounts they work from — email under your domain at minimum, plus whatever else the engagement touches, such as your ticketing system, client portal, and VPN or jump-host access. We deliberately do not use our own operations portal for white-label engagements, precisely because it is branded as ours.

Anything you issue us we treat as client-issued credentials: least privilege, used only for the engagement it was issued for, and returned or disabled at close. We confirm exactly which accounts are needed before testing starts, so nothing gets provisioned that will not be used.

Set up once, reuse indefinitely

Identity provisioning is a first-engagement cost, not a per-engagement one. Partners running steady volume keep a small standing set of accounts for their regular testers and add to it only when a new specialty is called in.

04 Subcontract Delivery

Not every partnership needs a brand exercise. When your client is comfortable knowing a specialist firm is doing the testing, subcontracting is faster to stand up, cheaper to run, and asks almost nothing of your operations team.

SC

We run the engagement, you stay in the loop

Disclosed subcontracting, managed end to end in our operations portal

You subcontract the assessment to us and we run it in **portal.brackish.io**. Your staff get named accounts scoped to the engagements they are on, so you can watch scope get agreed, findings land as they are confirmed, and the report get delivered — without chasing anyone for a status update.

WHAT YOU GET ACCESS TO

- ✓ The engagement's scope of record, as agreed and as amended.
- ✓ Findings as they are confirmed, risk-rated and evidenced — critical issues reported in real time, not held for the final report.
- ✓ Report delivery, revisions, and the final signed-off document.
- ✓ Messaging with the test team, in the engagement's own thread.
- ✓ Secure file exchange for credentials, architecture documents, and evidence.
- ✓ E-signature for the Statement of Work and Rules of Engagement.

WHO HOLDS ACCOUNTS

Portal accounts in this model are for **your** people. We do not provision your client directly — your firm stays their single point of contact, and you decide what is relayed and when.

Access is granted per engagement. A colleague added for one project sees that project, not your whole history with us.

Your client's side of the relationship stays yours

Where an engagement does call for client-side visibility, the portal does not expose our internal structure to it: which of us is an admin, a contractor, or read-only is not shown. Client-side accounts see the engagement role that actually matters — Lead Tester, Project Manager — and everyone at Brackish otherwise reads simply as internal staff.

05 The Operations Portal

Subcontracted engagements are managed at **portal.brackish.io** — the same system our own team runs every engagement from. There is no separate partner tool to learn, nothing to install, and nothing about an engagement living in an inbox where it cannot be found six months later.

ENGAGEMENT TRACKING

Status, dates, assigned team, and testing window for every project you are on — current and past.

SCOPE OF RECORD

What is in scope, what is explicitly out, and every amendment agreed along the way.

FINDINGS

Risk-rated with CVSS v3.1 and v4.0, mapped to OWASP, NIST, PTES, and CIS, with reproduction steps, evidence, and remediation guidance.

REPORT DELIVERY

Deliverables issued and versioned in the portal rather than mailed around as attachments.

MESSAGING

Conversation with the test team attached to the engagement it concerns, so context is not scattered across threads.

DOCUMENTS & SIGNATURES

Statements of Work and Rules of Engagement generated, reviewed, and signed in place.

Also included with engagements, in either model. A complimentary re-test of high and critical risk findings, requested within 60 days of final report delivery; an executive read-out with the engineering team; and a formal attestation letter suitable for customers and auditors, on request.

06 Reporting & Branding

The report is what your client judges the engagement by, so how it is branded is a decision you make rather than one you inherit. Three options, all carrying the same underlying content:

OPTION	WHAT YOU GET	TYPICAL MODEL
Brackish-branded	Our standard report on Brackish letterhead — executive summary, risk-rated findings, evidence, reproduction steps, and prioritized remediation guidance. Delivered as PDF, and as an editable document if your team wants to annotate it.	SUBCONTRACT

OPTION	WHAT YOU GET	TYPICAL MODEL
Generic / unbranded	The same content with our marks removed, in an editable document, for you to present however you choose. Useful when a client wants the technical substance without a third party's logo on it.	SUBCONTRACT WHITE LABEL
Your template and branding	You supply a report template and brand assets — logo, typography, palette, section structure, and any standing legal or scope language — and we author the engagement into it. The result is indistinguishable from a report your own team produced.	WHITE LABEL

Whichever option you pick, the substance does not change. Findings are risk-rated with CVSS v3.1 and v4.0, mapped to recognized standards (OWASP WSTG and ASVS, OWASP API Top 10 and MASVS, NIST, PTES, CIS), and written to be handed straight to the engineers who have to fix them. Every finding is manually verified — a scanner's unexamined opinion does not reach your client's report.

> **Supplying a template**
> Send it once, in whatever format you author in, along with a recent report you are happy with. We will come back with any questions about structure and severity language, then keep the template on file so later engagements need no further setup. If you do not have a template yet, start with the generic option and build one from the first delivery.

07 Service Catalog

Everything below is available under either partnership model. Services can be sold individually or combined into a program; each is scoped and reported separately.

SERVICE	WHAT IT COVERS	PRIMARY STANDARD
Web Application Penetration Test	Authenticated/unauthenticated testing of web apps, workflows, and business logic	OWASP WSTG / ASVS
API Penetration Test	REST, GraphQL, and other APIs — authz, data exposure, abuse	OWASP API Top 10
Mobile Application Penetration Test	iOS & Android apps, local storage, transport, and backend APIs	OWASP MASVS / MASTG

SERVICE	WHAT IT COVERS	PRIMARY STANDARD
AI / LLM Security Testing	LLM apps, AI workflows, prompt injection, and model-adjacent controls	OWASP LLM Top 10
Secure Source Code & DevOps Review	Manual code review plus SAST of security-critical components	OWASP ASVS / NIST SSDF
Vulnerability Assessment & Scanning	Broad automated discovery with manual validation across hosts, networks, and applications	NIST SP 800-115
External Infrastructure Test	Internet-facing perimeter, exposed services, and misconfigurations	PTES / NIST SP 800-115
Internal Network Test	Post-access lateral movement, AD, and privilege escalation	PTES / MITRE ATT&CK
Cloud Security Configuration Review	AWS / Azure / GCP architecture, IAM, and control review	CIS Benchmarks / Well-Architected
Configuration & Hardening Reviews	Host, server, container, device, and build hardening	CIS Benchmarks
Wireless Assessment	Wi-Fi security, rogue AP, segmentation, and client attacks	PTES / NIST SP 800-115
Red Team Operation	Objective-based, full-scope adversary emulation	MITRE ATT&CK
Purple Team Exercise	Collaborative attack + detection engineering with your blue team	MITRE ATT&CK
Social Engineering & Phishing	Phishing, vishing, and pretext-based human-layer testing	PTES

08 Commercial Model

Deliberately simple, because complicated partner economics are how partnerships quietly stop being used.

35%

of the engagement value is yours on a **white-label** engagement

20%

of the engagement value is yours on a **subcontract** engagement, where we run the engagement machinery

PRICED TOGETHER, PER ENGAGEMENT

We scope each assessment with you and agree its engagement value before the Statement of Work is signed, so you know your cost before you quote your client. The minimum engagement value is $4,500 — a one-day test.

YOUR CLIENT PRICE IS YOURS

You keep your share of the agreed engagement value, and anything you charge your client above it. What you charge your client is entirely your decision.

WE INVOICE YOU, NEVER YOUR CLIENT

We invoice your firm once the final report is delivered, payable net 45. The included re-test is never billed separately. We are not a party to your client contract and take no payment from your client.

NO MINIMUMS, NO CANCELLATION FEES

No volume minimum, no annual commitment, and no exclusivity in either direction. Bring us one engagement or twenty, and reschedule when your client needs to.

PAPERWORK, IN ORDER

- **Mutual NDA** — before scoping conversations touch anything about your clients.
- **Partner master agreement** — the standing terms between your firm and ours: confidentiality, intellectual property, liability, insurance, and non-solicitation of your clients.
- **Statement of Work** — per engagement: scope, deliverables, timeline, and fees.
- **Rules of Engagement** — per engagement: targets, testing windows, escalation contacts, and authorization to test.

The master agreement is signed once. After that, a new engagement needs only a Statement of Work and Rules of Engagement — both of which we generate and route for signature.

09 Onboarding

Standing the partnership up is a short exercise, and most of it happens once and never again.

01 Introduction call
Your service catalog, the clients you serve, and the engagements in front of you now. We will tell you plainly which model fits — including when the answer is that you do not need a partner for this one.

02 Mutual NDA
Executed before any conversation that touches a named client or a live environment.

03 Partner master agreement
The standing commercial and legal terms between our two firms, signed once.

04 Model setup
Subcontract: we create portal accounts for your team and walk them through it in a single call.
White label: you send us your report template and brand assets, and we agree the identities the assigned testers will need under your brand.

05 First engagement
Scoping call, agreed engagement value, Statement of Work and Rules of Engagement, then kickoff. A named project manager runs the engagement and stays your point of contact through delivery and re-test.

10 Frequently Asked Questions

What is white-label penetration testing?

It lets you offer expert security testing under your own brand. We perform the assessment, and every report and deliverable carries your company's logo and branding. Your client sees your firm, not ours.

How is subcontracting different?

In the subcontract model we are disclosed to your client as your testing partner, and the engagement runs in our operations portal with your team holding accounts on it. It is faster to stand up — no template work, no identity provisioning — and lighter on your operations team. The testing itself is identical.

Which model should we start with?

If you are selling testing as a standing line in your catalog and your positioning depends on it being yours, white label. If you have an engagement to deliver now and your client is comfortable knowing a specialist firm is doing the work, subcontract. Plenty of partners run both.

Will my clients know a third party performed the testing?

In the white-label model, no — all communication, documentation, and reporting is branded as yours. In the subcontract model, yes: we are named as your subcontractor, which most clients read as a positive signal that a specialist did the work.

Who is the program designed for?

MSPs, MSSPs, consultancies, and development agencies that want to offer offensive security without hiring and keeping an in-house testing team busy.

What types of testing do you provide?

The full suite: network, web application, API, cloud, mobile, IoT, wireless, physical, social engineering, AI/LLM, secure code review, and configuration reviews — each tailored to the environment in scope. Section 07 lists the catalog.

What do we have to provision for a white-label engagement?

Working identities for the assigned testers under your brand: email at minimum, plus whatever the engagement touches — ticketing, your client portal, VPN or jump-host access. We confirm the exact list before the engagement starts, and it is a first-engagement cost you reuse afterwards.

Do our clients get accounts in your portal?

Not by default — they are for your staff, and your firm stays your client's single point of contact. If an engagement is better served by giving your client direct visibility, we will set that up deliberately rather than by accident.

How does reporting work?

Three options — our branding, no branding, or yours; section 06 covers each. The content is identical in all three: risk-rated findings with CVSS v3.1 and v4.0, evidence, reproduction steps, and prioritized remediation guidance.

Do you re-test after our client remediates?

Yes. One re-test of high and critical risk findings is included in every engagement, requested within 60 days of final report delivery, and reported as a re-test letter.

Do you help our client fix what you find?

Every finding carries specific remediation guidance, and during the re-test window we answer written questions about it. We do not do hands-on remediation or engineering work; if your client needs more, it is scoped as its own engagement.

Will you go after our clients?

No — and the partner master agreement says so in writing. We will not solicit your clients, or take work from them directly even if they come to us, for the life of the agreement and twelve months after. Neither side hires the other's people either.

How quickly can you start?

Once the NDA and master agreement are in place, lead time on a new engagement depends on its scope and current scheduling. Ask on the scoping call and you will get a real date, not an aspiration.

How long until we have a report?

Critical findings reach you within 24 hours of confirmation. The draft report follows within 10 business days of testing ending, and the final within 5 business days of your comments.

How do you handle our clients' data?

Used only for the engagement, held in encrypted, access-controlled systems (or yours, on white label), and deleted 180 days after delivery. Credentials are least-privilege and returned at close; a security incident is reported to you within 72 hours.

11 Get Started

NEXT STEP

- Email us with your service catalog and the engagements you have in view.
- We recommend a model and walk you through it on a call.
- Execute the mutual NDA, then the partner master agreement.
- Scope your first engagement.

CONTACT

Brackish Security, LLC

Offensive Security

306 W Redwood St STE 201, Baltimore, MD 21201

Email: info@brackish.io

Phone: +1 (518) 629-0126

Web: brackish.io/partners · Portal: portal.brackish.io

OSCP | OSWE | OSEP | CISSP | **Active U.S. clearances held by select personnel**

Certifications and clearances are held across the testing team, our project managers hold PMP, and assigned personnel are confirmed at kickoff.